UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,708	02/05/2002	Luke David Jagger	NETAP021	1914

28875 7590 07/02/2007
Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
BILGRAMI, ASGHAR H	
ART UNIT	PAPER NUMBER
2143	
MAIL DATE	DELIVERY MODE
07/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/072,708
Filing Date: February 05, 2002
Appellant(s): JAGGER ET AL.

Kevin J. Zilka
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 8, 2007 appealing from the Office action mailed May 3, 2006.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences, which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

Amendment after final was filed.

(5) Summary of Claimed Subject Matter

The summary of the claimed subject matter is contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-8 & 10-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aronson et al (U.S. 6,654,787B1) in view of Leeds et al (U.S. 6,393,465B2). This rejection is set forth in a prior office action, mailed on May 3, 2006.

(7) Claims Appendix

The copy of the appealed claims contained in the appendix to the brief is correct.

(8) Evidence Relied Upon

6,654,787B1	Aronson et al.	10-2003
6,393,465B2	Leeds et al	05-2002

(9) Grounds of Rejection

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-8 & 10-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aronson et al (U.S. 6,654787 B1) and Leeds (U.S. 6,393,465 B2).

3. As per claims 1, 13 & 22 Aronson disclosed a system for generating a report on an unsolicited electronic message, the system comprising: a detector operable to detect a network address within an electronic message identified as an unsolicited message (col.4, lines 35-64), a host identifier operable to identify an authority hosting the network

address (col.4, lines 51-56 & col.5, lines 50-67); and a storage medium configured to at least temporarily store the identified network address and hosting authority (col.4, lines 57-67 & col.5, lines 1-8). However Aronson did not explicitly disclose a report generator operable to generate a report containing the identified network address and hosting authority.

In the same field of endeavor Leeds disclosed a host identifier operable to identify an authority hosting the network address; a report generator operable to generate a report containing the identified network address and hosting authority (Leeds, Abstract, col.3, lines 54-67, col.4, lines 1-35); wherein the hosting authority comprises identifying an owner of a network domain. (col.4, lines 60-67, col.5, lines 1-44 & col.6, lines 52-65).

At the time the invention was made it would have been obvious to one in the ordinary skill in the art to incorporate the capability of generating a report of containing the address sending unsolicited message and sending that report to the hosting authority as taught by Leeds in a system of detecting unsolicited messages as taught by Aronson in order to make the unsolicited electronic mail system more versatile and robust and result in an effective way to combat unsolicited messages to a user.

4. As per claims 2, 11, 17-19 & 24 Aronson-Leeds disclosed the method of claim 1 further comprising transmitting the report to a central managed service provider configured to forward, the report to the identified hosting authority (Leeds, col.4, lines 36-67, col.5, lines 1-44 & col.8, lines 34-57).

5. As per claims 3, 14 & 15 Aronson-Leeds disclosed the method of claim 1 wherein examining the message to identify a network address comprises identifying a URL (Aronson, col.5, lines 50-67).

6. As per claims 4, 20 & 25 Aronson-Leeds disclosed the method of claim 3 wherein identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL (Aronson, col.4, lines 57-67, col.5, lines 1-8 & col.5, lines 50-67).

7. As per claims5, 21 & 26 Aronson-Leeds disclosed the method of claim 3 further comprising comparing the identified URL to a database of legitimate URLs (Aronson, col.4, lines 57-67, col.5, lines 1-8 & col.5, lines 50-67).

8. As per claim 6 Aronson-Leeds disclosed the method of claim 5 further comprising updating the database based on electronic messages received (Aronson, col.6, lines 1-9).

9. As per claim 7 Aronson-Leeds disclosed the method of claim 3 wherein identifying the hosting authority comprises utilizing an Internet tool to locate a web server hosting the URL (Leeds, col.3, lines 54-67, col.4, lines 1-23, col.4, lines 60-67& col.5, lines 1-44).

10. As per claim 8 Aronson-Leeds disclosed the method of claim 7 wherein utilizing an Internet tool comprises utilizing WHOIS (Leeds, col.5, lines 21-25).

11. As per claims 10 & 16 Aronson-Leeds disclosed the method of claim 1 wherein identifying the hosting authority comprises identifying an Internet service provider (Leeds, col.3, lines 54-67, col.4, lines 1-23, col.4, lines 60-67& col.5, lines 1-44).

12. As per claim 12 Aronson-Leeds disclosed the method of claim 1 further comprising at least temporarily saving the report and transmitting the report to the identified hosting authority at the end of a specified period (Leeds, col.5, lines 38-44)

13. As per claim 23 Aronson-Leeds disclosed the computer product of claim 22 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and a data signal embodied in a carrier wave Leeds, col.3, lines 10-36).

14. As per claim 27, 28, 29, 30 & 31 Aronson-Leeds disclosed the method of claim 1 wherein identifying the hosting authority further comprises is identifying an address, an administrative contact name, an administrative contact telephone number, and name of at least one server associated with the hosting authority (Leeds, col.4, lines 37-67 & col.5, lines 1-44).

(10) Response to Arguments

The applicant argues the following issues regarding independent **claims 1, 3 & 22** to support his position against the prior arts Aronson et al (U.S. 6,654,787B1) and Leeds et al (U.S. 6,393,465B2).

(A) Rejection under 35 U.S.C 103(a) with regards to claims 1, 3, 7-8, 13-15, 17 and 27-28

Issue 1: The appellant alleges (on pages 12 & 13) that neither Leeds nor Aronson disclose the limitation in all the independent claims which states "identifying the authority hosting the network address".

Appellant on page 7 lines 12-16 of the application's specification states " the present invention provides a method and system for generating a report upon detection of unsolicited or SPAM electronic mail ('e-MAIL') messages. The report is preferably automatically generated upon detection of an unsolicited e-mail. In one embodiment, the system sends the report to the **relevant authority (e.g., Internet Service Provider (ISP) or backbone provider hosting the spammer)**."

From the above excerpt it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. e-mail address) can in fact be the Internet service provider (ISP).

Most common Internet service providers (ISP) include AOL, Yahoo, Hotmail, Comcast and Google etc.

Examiner notes that it not possible to send e-mail or electronic mail without the presence of an Internet Service Provider. Therefore in a classic example when a spammer sends an e-mail containing SPAM he or she sends it via a hosting authority I.E an ISP. For example a SPAM mail coming from, Spammer@aol.com. In this address "Spammer" signifies the unique address that identifies the address of the spammer whereas, "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.

Both Aronson and Leeds disclose methods of identifying and controlling e-mails that contain SPAM along with identifying the sources that send the SPAM. Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mail is SPAM mail or not. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent. Based on the verification response that is received in response to the verification request, the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail. Incoming messages (e-mails) are automatically scanned and parsed either (1) at a server located at an Internet Service Provider (prior to delivery to the intended ultimate recipient, (2) at a LAN-based receiving station or (3) at the actual ultimate recipient's mail machine i.e., local to the user." Leeds further elaborates the analysis process on col.4, lines 65-67 and states " The line: From 48941493@notarealaddress.com is broken down into a user id (48941439) and a host name {hosting authority} notarealaddress.com. Leeds on col5, lines 13-33 further describes using the UNIX "WHOIS" command to identify and determine if a site (or hosting authority) actually exists. Therefore Leeds clearly discloses identifying the hosting authority that is hosting the network address. Finally examiner notes that appellant in his own specification on page 12 lines 9-14 has described the same "WHOIS" method to identify the ISP (hosting authority) associated with the network address.

Issue 2: The appellant (on page 14) alleges that Leeds fails to disclose or even suggest, "generating a report containing the identified network addresses and hosting authority".

As to appellant's argument, in addition to identifying the network address and hosting authority (as described in issue 1) Leeds discloses maintaining (1) a list of mail of certain mail providers (i.e. hosting authorities/ISPs) known to be an origination point of junk e-mail (SPAM), (2) a dictionary of certain content frequently found in junk e-mail, and (3) a learning knowledge base that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds discloses that the rules are continually modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities can be called a report, which can be sent or transmitted to related authorities for appropriate action.

Issue 3: **The appellant (on page. 15) alleges that there is no motivation to combine the prior art references.**

As to appellant's arguments both Aronson and Leeds disclose methods of identifying and controlling e-mails that contain SPAM along with identifying the sources that send the SPAM. Leeds in addition to blocking the junk-mail (SPAM) has a learning knowledge base that continually maintains a list of hosting authorities and addresses that are culprits of sending junk-mail (SPAM) to prevent future SPAM mails from such hosts and addresses (col.4, lines 24-35). Therefore it is logical and obvious to combine the two references together to anticipate applicant's invention.

(B) Rejection under 35 U.S.C 103(a) with regards to claims 2, 18 & 24

Issue 1: Appellant argues (on page.15) and states the prior art does not teach the dependent claim "transmitting the generated report to the identified hosting authority".

Leeds on col.4, lines 27-35 discloses a "learning knowledge base" that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds disclosed that the rules are continually modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action.
As to applicants argument Leeds discloses sending verification e-mail to the sender with a respective host authority. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent (Please also read col.4, lines 65-67). It would have been obvious to one in the ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com

or any hosting authority administering the hosting along with list as an attachment disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM.

(C) Rejection under 35 U.S.C 103(a) with regards to dependent claims 4, 5 & 6

Issue 1: Appellant argued (on page 17) that neither Aronson nor Leeds disclose, "comparing the identified URL to a database of legitimate URL".

As to appellant's argument Aronson on col.1, lines 52-55 discloses a well know technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses). On col.5, a line 50-67 discloses employing rule handling filter modules 720 through 760 to control SPAM. Aronson further states "**RS(c) may be an inclusion list**. Other contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g. based on phone numbers, URL's, addresses etc). It should noted that **all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network**."

(D) Rejection under 35 U.S.C 103(a) with regards to dependent claim 10

Issue 1: **Appellant (on page.17) argued that Leeds fails to disclose or even suggest "wherein identifying the hosting authority comprises identifying the Internet Service provider".**

Appellants on page 7 lines 12-16 of the application's specification states " the present invention provides a method and system for generating a report upon detection of unsolicited or SPAM electronic mail ('e-MAIL') messages. The report is preferably automatically generated upon detection of an unsolicited e-mail. In one embodiment, the system sends the report to the **relevant authority (e.g., Internet Service Provider (ISP) or backbone provider hosting the spammer)**."

From the above excerpt it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. e-mail address) can in fact be the Internet service provider (ISP). Most common Internet service providers (ISP) include AOL, Yahoo, Hotmail, Comcast and Google etc.

Examiner notes that it not possible to send e-mail or electronic mail without the presence of an Internet Service Provider. Therefore in a classic example when a spammer sends an e-mail containing SPAM he or she sends it via a hosting authority I.E an ISP. For example a SPAM mail coming from, Spammer@aol.com. In this address "Spammer" signifies the unique address that identifies the address of the spammer whereas, "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.

Both Aronson and Leeds disclose methods of identifying and controlling e-mails that contain SPAM along with identifying the sources that send the SPAM. Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mail is SPAM mail or not. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent. Based on the verification response that is received in response to the verification request, the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail. Incoming messages (e-mails) are automatically scanned and parsed either (1) at a server located at an Internet Service Provider (prior to delivery to the intended ultimate recipient, (2) at a LAN-based receiving station or (3) at the actual ultimate recipient's mail machine i.e., local to the user." Leeds further elaborates the analysis process on col.4, lines 65-67 and states " The line: From 48941493@notarealaddress.com is broken down into a user id (48941439) and a host name {hosting authority} notarealaddress.com."

(E) Rejection under 35 U.S.C 103(a) with regards to dependent claim 11

Issue 1: The appellant alleges (on page 18) alleges that Leeds does not disclose, "transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority".

Leeds on col.4, lines 27-35 discloses a "learning knowledge base" that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds disclosed that the rules are continually modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action.
As to applicants argument Leeds discloses sending verification e-mail to the sender with a respective host authority. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent (Please also read col.4, lines 65-67). It would have been obvious to one in the

ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with list as an attachment disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM.

(F) Rejection under 35 U.S.C 103(a) with regards to dependent claim 12

Issue 1: Applicant argued (on page 18) alleges that Leeds does not disclose "transmitting the report to the identified hosting authority at the end of a specified period".

Leeds on col.4, lines 27-35 discloses a "learning knowledge base" that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds disclosed that the rules are continually modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action.
As to applicants argument Leeds discloses sending verification e-mail to the sender with a respective host authority. On col.3, lines 57-67 Leeds states, "The method and system

begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent (Please also read col.4, lines 65-67). It would have been obvious to one in the ordinary skill in the art to send an e-mail in the similar way at a particular time to the administrator@aol.com or any hosting authority administering the hosting along with list as an attachment disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM.

(G) Rejection under 35 U.S.C 103(a) with regards to dependent claim 16

Issue 1: **The Appellant (on page 19) alleges that Leeds fail to even suggest a technique "wherein the hosting authority is an Internet service provider".**

As to appellant's argument Appellants on page 7 lines 12-16 of the application's specification states " the present invention provides a method and system for generating a report upon detection of unsolicited or SPAM electronic mail ('e-MAIL') messages. The report is preferably automatically generated upon detection of an unsolicited e-mail. In one embodiment, the system sends the report to the **relevant authority (e.g., Internet Service Provider (ISP) or backbone provider hosting the spammer).**" From the above excerpt it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. e-mail address) can in fact be the Internet service provider (ISP).

Most common Internet service providers (ISP) include AOL, Yahoo, Hotmail, Comcast and Google etc.

Examiner notes that it not possible to send e-mail or electronic mail without the presence of an Internet Service Provider. Therefore in a classic example when a spammer sends an e-mail containing SPAM he or she sends it via a hosting authority I.E an ISP. For example a SPAM mail coming from, Spammer@aol.com. In this address "Spammer" signifies the unique address that identifies the address of the spammer whereas, "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.

Both Aronson and Leeds disclose methods of identifying and controlling e-mails that contain SPAM along with identifying the sources that send the SPAM. Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mail is SPAM mail or not. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent. Based on the verification response that is received in response to the verification request, the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail. Incoming messages (e-mails) are automatically scanned and parsed either (1) at a server located at an Internet Service Provider (prior to delivery to the intended ultimate recipient, (2) at a LAN-based receiving station or (3) at the actual ultimate recipient's mail machine i.e., local to the user." Leeds further elaborates the analysis process on col.4, lines 65-67 and states " The line: From 48941493@notarealaddress.com is broken down into a user id (48941439) and a host name {hosting authority} notarealaddress.com. Leeds on col5, lines 13-33 further describes using the UNIX "WHOIS" command to identify and determine if a site (or hosting authority) actually exists. Therefore Leeds clearly discloses identifying the hosting authority that is hosting the network address.

(H) Rejection under 35 U.S.C 103(a) with regards to dependent claim 19

Issue 1: **The Appellant (on page.20) alleges that Leeds does not disclose, "Wherein the processor is configured to report to a central managed service provider".**

Leeds on col.4, lines 27-35 discloses a "learning knowledge base" that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds disclosed that the rules are continually modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action.

As to applicants argument Leeds discloses sending verification e-mail to the sender with a respective host authority. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent (Please also read col.4, lines 65-67). It would have been obvious to one in the ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any centrally managing hosting authority administering the hosting along with list as an attachemnt disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM.

(I) Rejection under 35 U.S.C 103(a) with regards to dependent claim 20

Issue 1: The Appellant (on page.20) alleges that Aronson fails to disclose "database containing search terms used to identify the network address within the text of the electronic message".

As to appellant's argument Aronson on col.1, lines 52-55 discloses a well know technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses). On col.5, a line 50-67 discloses employing rule handling filter modules 720 through 760 to control SPAM. Aronson further states "**RS(c) may be an inclusion list**. Other contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g. based on phone numbers, URL's, addresses etc). It should noted that **all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network**." Aronson further elaborates one of the rules and on col.6, lines 47-52 states, "For example, a rule which is geared towards screening e-mail messages containing sexual content (e.g., in a home where children use the computer) which filters e-mails based on the keywords "sex" and "free" may be given a weighted value of 10 on a scale from 1 to 10."

(J) Rejection under 35 U.S.C 103(a) with regards to dependent claim 21

Issue 1: **The Appellant (on page.21) alleges that Aronson fails to disclose "database containing a list of trusted network addresses".**

As to appellant's argument Aronson on col.1, lines 52-55 discloses a well know technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses). On col.5, a line 50-67 discloses employing rule handling filter modules 720 through 760 to control SPAM. Aronson further states "**RS(c) may be an inclusion list**. Other contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g. based on phone numbers, URL's, addresses etc). It should noted that **all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network**."

(K) Rejection under 35 U.S.C 103(a) with regards to independent claim 22 & dependent 23

Issue 1: **The Appellant (on page.22) alleges that Aronson and Leeds reference are only related to a host computer associated with a sender of the electronic mail and not identifying the authority hosting the network address as claimed by the appellant.**

Appellant on page 7 lines 12-16 of the application's specification states " the present invention provides a method and system for generating a report upon detection of unsolicited or SPAM electronic mail ('e-MAIL') messages. The report is preferably automatically generated upon detection of an unsolicited e-mail. In one embodiment, the system sends the report to the **relevant authority (e.g., Internet Service Provider (ISP) or backbone provider hosting the spammer).**"

From the above excerpt it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. e-mail address) can in fact be the Internet service provider (ISP). Most common Internet service providers (ISP) include AOL, Yahoo, Hotmail, Comcast and Google etc.

Examiner notes that it not possible to send e-mail or electronic mail without the presence of an Internet Service Provider. Therefore in a classic example when a spammer sends an e-mail containing SPAM he or she sends it via a hosting authority I.E an ISP. For example a SPAM mail coming from, Spammer@aol.com. In this address "Spammer" signifies the unique address that identifies the address of the spammer whereas, "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.

Both Aronson and Leeds disclose methods of identifying and controlling e-mails that contain SPAM along with identifying the sources that send the SPAM. Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mail is SPAM mail or not. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information

{I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent. Based on the verification response that is received in response to the verification request, the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail. Incoming messages (e-mails) are automatically scanned and parsed either (1) at a server located at an Internet Service Provider (prior to delivery to the intended ultimate recipient, (2) at a LAN-based receiving station or (3) at the actual ultimate recipient's mail machine i.e., local to the user." Leeds further elaborates the analysis process on col.4, lines 65-67 and states " The line: From 48941493@notarealaddress.com is broken down into a user id (48941439) and a host name {hosting authority} notarealaddress.com. Leeds on col5, lines 13-33 further describes using the UNIX "WHOIS" command to identify and determine if a site (or hosting authority) actually exists. Therefore Leeds clearly discloses identifying the hosting authority that is hosting the network address.

(L) Rejection under 35 U.S.C 103(a) with regards to dependent claim 25

Issue 1: The Appellant (on page.25) alleges that Aronson fails to disclose or suggest "code that compares text within the electronic message to a database of words to locate the network address within the text".

As to appellant's argument Aronson on col.1, lines 52-55 discloses a well know technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses). On col.5, a line 50-67 discloses employing rule handling filter modules 720 through 760 to control SPAM. Aronson further states "**RS(c) may be an inclusion list**. Other contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g. based on phone numbers, **URL's, addresses** etc). It should noted that **all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network**."

(M) Rejection under 35 U.S.C 103(a) with regards to dependent claim 26

Issue 1: The Appellant (on page.26) alleges that Aronson fails to disclose or suggest "code that compares the identified network address with trusted network address".

As to appellant's argument Aronson on col.1, lines 52-55 discloses a well know technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses). On col.5, a line 50-67 discloses employing rule handling filter modules 720 through 760 to control SPAM. Aronson further states "**RS(c) may be an inclusion list**. Other contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g. based on phone numbers, **URL's, addresses** etc). It should noted that **all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network**."

(N) ***Rejection under 35 U.S.C 103(a) with regards to dependent claim 29***

Issue 1: The Appellant (on page.26) alleges that Leeds fail to disclose, "Wherein the report is utilized to generate an electronic mail message to be sent to the identified organization."

Leeds on col.4, lines 27-35 discloses a "learning knowledge base" that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds disclosed that the rules are continually modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action.

As to applicants argument Leeds discloses sending verification e-mail to the sender with a respective host authority. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent (Please also read col.4, lines 65-67). It would have been obvious to one in the ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any organization hosting authority administering the hosting along with list as an attachment disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM.

(O) ***Rejection under 35 U.S.C 103(a) with regards to dependent claim 30***

Issue 1: **The Appellant (on page.27) alleges that Leeds fail to disclose, "wherein identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address with unsolicited messages."**

As to appellant's argument Aronson on col.1, lines 52-55 discloses a well know technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses). On col.5, a line 50-67 discloses employing rule handling filter modules 720 through 760 to control SPAM. Aronson further states "**RS(c) may be an inclusion list**. Other contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) **misspelling analysis** (unwanted e-mail often contains misspelled words); (4) **word or letter combination analysis**; (5) technical or legal RFC822 header compliance; and (6) **feature extraction & analysis** (e.g. based on phone numbers, **URL's, addresses** etc). It should noted that **all of the rule handling filter modules described herein**

may be combined or applied over a distributed array of filters throughout a network."

(P) Rejection under 35 U.S.C 103(a) with regards to dependent claim 31

Issue 1: **The Appellant (on page.26) alleges that Leeds fail to disclose, "wherein the report includes disclaimer information and user definable text".**

Leeds on col.4, lines 27-35 discloses a "learning knowledge base" that creates its own rules to ascertain prior junk e-mail characteristics and subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered. Leeds disclosed that the rules are continually modified and maintained i.e. **stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive**, thereby effectively and intelligently mitigating the delivery of Junk-mail (SPAM). Hence the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action.

Additionally Leeds discloses sending verification e-mail to the sender with a respective host authority. On col.3, lines 57-67 Leeds states, "The method and system begins by analyzing the origins and transmission paths of the messages. The sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent (Please also read col.4, lines 65-67). It would have been obvious to one in the ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with list as an attachment disclosed by Leeds containing a disclaimer information and user definable text (i.e. network address uniquely identifying the user).

(11) Related Proceedings Appendix

None.

Respectfully submitted,

Asghar Bilgrami
Patent Examiner
Art Unit 2143
June 19, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100